UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/659,864	09/12/2000	J. Leslie Vogel III	0044860.P2436	5866

7590 02/17/2006

Sheryl Sue Holloway
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard &th Floor
Los Angeles, CA 90025

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/659,864	**Applicant(s)** VOGEL, J. LESLIE	
	Examiner Tongoc Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on November 28, 2005. Claims 1, 16, 21, 26, 31, 36, 42 and 46 have been amended. Claims 1-51 are pending.

Response to Arguments

2. Applicant's arguments filed November 28, 2005 have been fully considered but they are not persuasive.

In response to Applicant's similar remark to claim rejection under U.S.C. 102 (a) and U.S.C. 103 (remark, pages 14 and 15) have been addressed below in the claim rejection under U.S.C. 112.

In response to Applicant's assertion that *"Lewis discloses two different devices (key distribution server and access point) providing two different layers of encryption to secure a network, the Examiner has combined Lewis' key distribution server and access point into a single device to read on Applicant's claimed access point*" (remark, page 15). Examiner notes that in Fig. 1 and Fig. 2, Lewis teaches an encryption engine resides in an access point (see col. 15, lines 25-34, Fig. 1, block 54, Fig. 2, block 118).

In response to Applicant's assertion that "*Schneier is directed toward various cryptographic processes and contains no disclosure related to access points that send a security preference as claimed in the independent claims, from which claims 4-8, 18, 23, 28, 33, 39 and 49 depend"* (remark, page 16, 3rd paragraph). However, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Lewis discloses message transmitted between the access point and the station are encrypted via the encryption engines on both sides. Therefore, it would have been obvious that Schneier's self distributed key technique would have been an obvious choice to be implemented in Lewis systems so that it ensure that the keys used to encrypt the message does not required to be transmitted between the access point and the station (Fig. 2, blocks 118 and block 94).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 16, 21, 26, 31, 36, 42 and 46 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The independent claims recite "wherein the security preference specifics one authentication protocol from a set of authentication protocols supported by the access point". However, in the Specification, Applicant discloses "*the station sends a request for security preference for access point to the access point. The access point sends the security preference in response to the request when the access point an support the channel. When the security preference is shared key, the station generates authentication information using a first key and sends the authentication information to the access point*" (page 4, lines 11-16); *"[t]he request message also includes an inquiry regarding the security preferences of the AP. The response received (block 303) will indicate whether a connection is available (block 305) and if so, the type of security preference (block 307). If there is no connection available, or if the security preference is not "shared key," the security method 300 exits. It will be appreciated that an available connection using a different security preference can be established through other methods not germane to the present invention"* (page 15, lines 7-13). In this portion of the Specification, there is no mention of the security preference represent a selected authentication protocol being selected from a set of plurality of authentication protocol. Furthermore, the reference of Fig. 3A, blocks 303, 305 and 307 for the station or Fig. 4A blocks 401, 403. 405 and 407 for the access point also fail to teach this limitation. Blocks 305 and 307 for the station merely indicated if the conditional steps of whether the connection available, if no, no connection is established, else, if the shared key available, implement key exchanged, else, no connection is established. Blocks 403 and 405 merely indicated the conditional steps of after receiving the request, check if there is an available connection, if true, response by sending security reference to the station. There is no reference that the access point, for example, determine from a plurality of authentication protocol and response with a preferred preference from those plurality of protocol to the station. The flow chart of 403 merely check if there is connection available, then response with a response of security preference, the similar teaching is also found on page 16 in the Specification. Therefore, because either the Specification or the flow chart in the drawings fail to specify the step where access point responding to the request by determining a security preference from a plurality of authentication protocols or how the step of selection is made from a pool of available authentication protocols. Checking for connection availability and response with the request of preference as indicated in the description of Fig. 4 of Specification, *"[t]he AP method receives the request from the station at block 401, determines if there is an available connection (block 403) and responds with the AP security preferences if so (block 405). The AP computer next performs a key exchange method at block 407 when required..." (Specification, page 16, 3rd paragraph),* therefore fail to provide necessary steps to support the amended claim. In light of the foregoing rationale, the amended limitations are not given patentable weight.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1, 16, 21, 26, 31, 36, 42 and 46 are rejected under 35 U.S.C. 102(a) as being anticipated by Patiyoot et al. ("Technique for authentication protocols and key distribution on wireless ATM networks", ACM SIGOPS Operating System Review, Volume 32, Issue 4, October 1998).

In respect to claim 1, Lewis discloses a computerized method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point through a setup connection, a request for a security preference for the access point (WAT- station; WAS- access point pages 25-27, 2.2-4.2.1),

sending, by the access point to the station through the setup connection, the security preference in response to the request when the access point can support the channel (page 27, 4.1 and 4.2.1)

sending, by the station to the access point through the setup connection, the authentication information (page 27, 4.1 and 4.2.1);

validating, by the access point, the station using the authentication information; encrypting, by the access point, the channel key using a second key when the station is validated (page 27, 4.1 and 4.2.1);

sending, by the access point to the station through the setup connection, the encrypted channel key (page 27, 4.2.1);

decrypting, by the station, channel key in response to receiving the encrypted channel key; and sending, by the station to the access point, data encrypted with the channel key to establish the channel (page 27, 4.2.1).

In respect to claims 16, 21, 26, 31, 36, 42 and 46, the claimed limitations are similar to claim 1. Therefore, the claims are rejected based on the similar rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent No. 6,526,506) in view of Quick Jr. (U.S. Patent No. 6,178,506, hereinafter Quick)

In respect to claim 1, Lewis discloses a computerized method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point through a setup connection, a request for a security preference for the access point (see Lewis, Fig. 6 and col. 10, line 46-col. 11, line 40);

sending, by the access point to the station through the setup connection, the security preference in response to the request when the access point can support the channel (see Lewis, col. 12, line 60-col. 13, line 15);

sending, by the station to the access point through the setup connection, the authentication information (see Lewis, col. 4, lines 27-42);

validating, by the access point, the station using the authentication

information; encrypting, by the access point, the channel key using a second key

when the station is validated (see Lewis, col. 4, lines 27-42 and col. 5, lines 29-41);

sending, by the access point to the station through the setup connection, the encrypted channel key (see Lewis, col. 5, lines 29-41);

decrypting, by the station, channel key in response to receiving the

encrypted channel key; and sending, by the station to the access point, data encrypted with the channel key to establish the channel (see Lewis, col. 5, line 10-col. 6, line 17).

Lewis discloses the mobile terminal sending authentication information (registering) with the access point (see Lewis, col. 4, lines 28-35) but does not explicitly discloses encrypting the authentication information. However, Quick discloses encrypting authentication information from mobile terminal to access point (Quick, col. 3, lines 1-10). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Quick's encrypting the authentication information with the teaching of Lewis' registering the mobile terminal with the access point in order to protect the user identification and password from compromise during the registration process (Quick, col. 2, lines 46-49).

In respect to claim 2, Lewis and Quick disclose the method of claim 1, wherein the first and second keys are a self-distributed key (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 3, Lewis discloses the method of claim 1, Lewis wherein the first and second keys are a self distributed key and further comprising:

generating, by the access point, the self-distributed key using a security algorithm when the security preference is shared key; generating, by the station and sending to the access point, a first value using the security algorithm in response to receiving the security preference of shared key; generating, by the access point, and sending to the station, a second value using the security algorithm and the first value in response to receiving the first value; and calculating, by the station, the self-distributed key using the security algorithm and the second value in response to receiving the second value (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 9, Lewis and Quick disclose the method of claim 2 further comprising:

encrypting, by the station, a name and password with the first key to generate the authentication information; and decrypting, by the access point, the name and password to validate the station (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 10, Lewis and Quick disclose the method of claim 2 further comprising:

sending, by the access point to the station, a challenge; encrypting, by the station, the challenge with the first key to generate the authentication information; encrypting, by the access point, the challenge with the first key; and comparing, by the access point, the authentication information with the challenge encrypted by the access point with the first key to validate the station (see Quick, col. 4, line 45-col. 5, line 8)

In respect to claim 11, Lewis and Quick disclose the method of claim 1, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station (see Quick, col. 4, line 45 -col. 5, line 8).

In respect to claim 12, Lewis and Quick disclose the method of claim 11 further comprising:

sending, by the access point to the station, the first key; and.

sending, by the station to the access point, the second key (see Quick col. 4, line 45-col. 5, line 8)

In respect to claim 13, Lewis and Quick disclose the method of claim 12, wherein the second key is sent to the access point when the request for the security preference is sent by the station (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 14, Lewis and Quick disclose the method of claim 12, wherein the first key is sent to the station when the security preference is sent by the access point (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 15, Lewis discloses the method of claim 1, wherein establishing the channel creates a standard wired equivalent privacy (WEP) network, and the station and the access point exchange messages conforming to a format required by the standard that defines a WEP network to establish the WEP network (see Lewis, col. 2, lines 18-43).

In respect to claim 16, 21, 26, 31 and 36-37, 40, 42-47 and 50, the claim limitations are substantially similar to claim 1. Therefore, claims 16, 21, 26, 31, 36-37, 40, 42-47 and 50 are rejected based on the similar rationale.

In respect to claim 17, the claim limitation is substantially similar to claim 3. Therefore, claim 17 is rejected based on the similar rationale.

In respect to claim 19, the method of claim 16 further comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key (see Lewis, col. 5, line 10-col. 6, line 17).

In respect to claims 20, 25, 30, 35, 41 and 51, the claim limitations are substantially similar to claim 11. Therefore, claims 20, 25, 30 and 35 are rejected based on the similar rationale.

In respect to claims 24, 29 and 34, the claim limitations are substantially similar to claim 19. Therefore, claims 24, 29 and 34 are rejected based on the similar rationale.

In respect to claim 22, the claim limitation is substantially similar to claim 3. Therefore, claim 22 is rejected based on the similar rationale.

In respect to claim 27, the claim limitation is substantially similar to claim 17. Therefore claim 27 is rejected based on the similar rationale.

In respect to claim 32, the claim limitation is substantially similar to claim 22. Therefore, claim 32 is rejected based on the similar rationale.

In respect to claim 38, Lewis and Quick disclose the secure wireless network of claim 37, wherein access point if further operable for encrypting the shared channel key using a self-distributed key for sending to the station and the station is further operable for decrypting the shared channel key upon receipt (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 48, the claim limitation is substantially similar to claim 38. Therefore, claim 48 is rejected based on the similar rationale.

6. Claims 4-8, 18, 23, 28, 33, 39 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent No. 6,526,506) in view of Quick Jr. (U.S. Patent No. 6,178,506, hereinafter Quick) and further in view of Schneier

("Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 1996, hereinafter Schneier).

In respect to claim 4, Lewis and Quick disclose the method of claim 3. Lewis and Quick do not disclose but Schneier discloses wherein the security algorithm is g mod p and further comprising: obtaining, by the access point, integers x, g and p to generate the self-distributed key k = g" mod p; obtaining, by the station, the integers g and p, and an integer y to generate the first value Y = g' mod p; generating, by the access point, the second value X = Yx mod p; and setting, by the, z equal to y -'to calculate the self-distributed key k = XZ mod p (see Schneier, page 515, Hughes). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Schneier with the teaching of Lewis's wireless communication between mobile and access point and Quick's Diffie-Hellman's protocol with Schneier's teaching of Hughes' protocol so that key can be computed before any interaction between the mobile station and the access point (see Schneier, page 515, Hughes and Key Exchange Without Exchanging Keys).

In respect to claim 5, Lewis, Quick and Schneier disclose the method of claim 4 wherein obtaining, by the station, the integers g and p comprises:

sending, by the access point (Bob) to the station (Alice), the integers for g and p (see Schneier, page 515, g and n).

In respect to claim 6, Lewis, Quick and Schneier disclose the method of claim 5, wherein the integers for g and p (g and n) are sent to the station (Alice) when the security preferences are sent by the access point (Bob) (see Schneier, page 515, Hughes).

In respect to claim 7, Lewis, Quick and Schneier disclose the method of claim 5, wherein g and p are sent to the station when a user name and password for the station are registered with the access point (see Quick, col. 4, line 60 to col. 5, line 8).

In respect to claim 8, Lewis, Quick and Schneier discloses the method of claim 4 further comprising:

publishing, by the access point, the integers g and p for a set of stations (see Schneier, page 515).

In respect to claims 18, 23, 28 and 33, the claim limitations are substantially similar to claim 4. Therefore, claims 18, 23, 28 and 33 are rejected based on the similar rationale.

In respect to claim 39, Lewis and Quick disclose the secure wireless network of claim 38. Lewis and Quick do not disclose but Schneier discloses wherein the station and the access point are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol (see Schneier, page 515, Hughes). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Schneier with the teaching of Lewis's wireless communication between mobile and access point and Quick's Diffie-Hellman's protocol with Schneier's teaching of Hughes' protocol so that key can be computed before any interaction between the mobile station and the access point (see Schneier, page 515, Hughes and Key Exchange Without Exchanging Keys).

In respect to claim 49, the claim limitation is substantially similar to claim 39. Therefore, claim 49 is rejected based on the similar rationale.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

February 13, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER